Carnegie Mellon
Software Engineering Institute

Managing for Enterprise Security

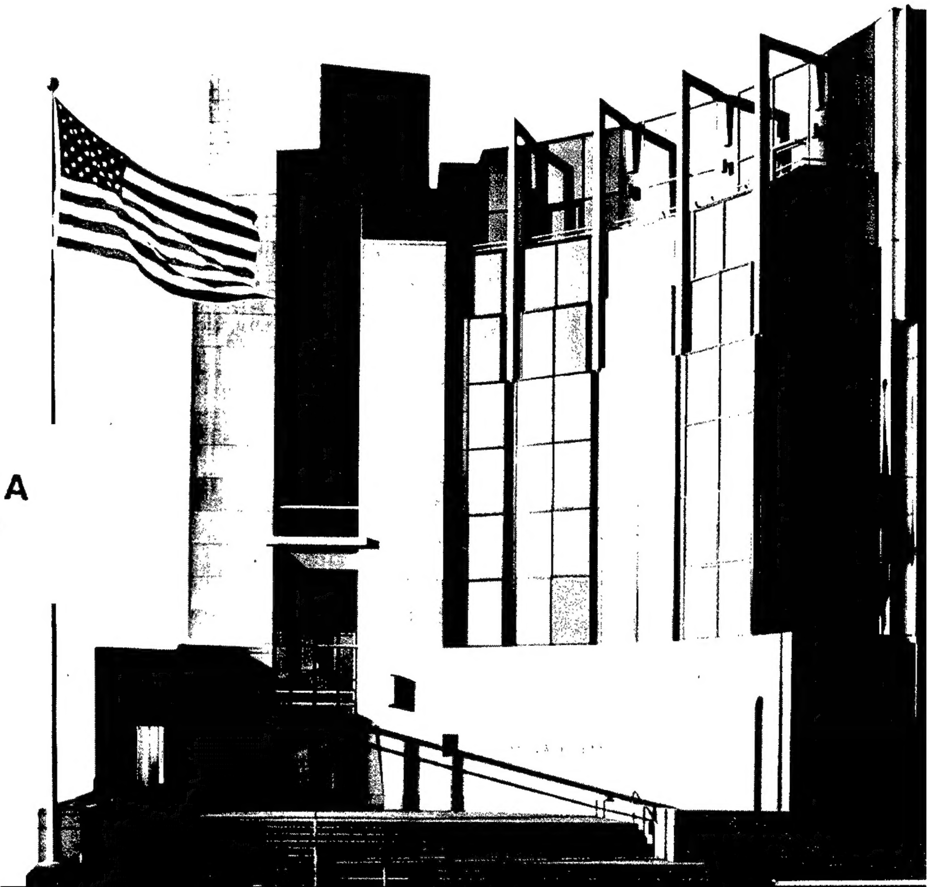
Author
Richard A. Caralli

Principal Contributors
Julia H. Allen
James F. Stevens
Bradford J. Willke
William R. Wilson

December 2004

Networked Systems Survivability Program

Technical Note
CMU/SEI-2004-TN-046



Managing for Enterprise Security

Author
Richard A. Caralli

Principal Contributors
Julia H. Allen
James F. Stevens
Bradford J. Willke
William R. Wilson

December 2004

Networked Systems Survivability Program

Technical Note
CMU/SEI-2004-TN-046

This work is sponsored by the U.S. Department of Defense.

The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Contents

List of Tables

To the Reader

Our work in the Networked Systems Survivability (NSS) program at the Carnegie Mellon® Software Engineering Institute (SEI) brings us in close contact with a broad array of organizations that seek to improve their security capabilities. We actively coach, mentor, and train many of these organizations to help them more effectively achieve their security goals. We develop and transition new security methodologies and technologies to empower organizations to take control of their security programs and activities. Yet, through all of this, we are constantly reminded that sustained, measurable achievement of security goals is still elusive for most organizations, even though they are working harder and committing previously unheard-of levels of resources to the task.

The logical next step in our work is to explore this problem more thoroughly and to identify practical solutions. Essentially, we seek to ask and answer the following question: What's missing from common approaches to security that would enable organizations to achieve and sustain an acceptable, adequate, predictable level of security that is commensurate with meeting their mission? Answering this question requires an exploration and discussion of the current challenges that organizations face. Our experience tells us that IT-centric approaches to security are too narrow and fail to mobilize the entire organization to manage and solve what is essentially a business problem. But what other barriers and challenges do organizations face in improving their security efforts? What prior notions about security must be challenged and overcome? And what are the foundations of a solution that would effectively help an organization to improve its security efforts?

Our objective in this technical note is to present the interim results of our work in exploring these issues and in working toward solutions. We offer a view of the changing environment in which security must be performed and, from our field work and research, we itemize characteristics of common existing approaches to security that limit effectiveness and success. A "desired state" as a security target for the organization is outlined, and the organizational transformation that we believe is essential for approaching security on an organizational scale is presented. Finally, we provide a description of our current work in exploring solutions that we believe will enable this transformation.

The intended audience for this document is not only the vast array of security practitioners (chief security officers, information security managers, and security administrators), but strategic planners, risk managers, and other business personnel who are confronting an increasingly hostile risk environment while trying to accomplish their organizational goals

® Carnegie Mellon is registered in the U. S. Patent and Trademark Office by Carnegie Mellon University.

and mission. Readers who are interested in taking a step back to examine their security challenges more fully should start with the introduction in Section 1 and continue through the document. However, for those readers who are familiar with SEI work that positions security in the context of survivability, a logical start would be in Section 3 where we begin to explore elements of making this shift as well as the expansion of security and survivability to the concept of organizational resiliency.

Our primary objective in developing this technical note is not to redefine the term "enterprise security management" but to introduce concepts and elements that characterize a new way of thinking about security from a managerial perspective. In future technical notes, we plan to provide more detailed updates on the practical deployment of these concepts and elements in field work and continuing research.

In addition, our work in enterprise security management is not about creating a new set of practices, standards, or guidelines for security. We recognize that there are plenty of these available at every turn. On the contrary, our interest lies in enabling organizations to manage security in a systematic, predictable, and adaptable way that fits their unique strategic drivers regardless of which practices, standards, or guidelines they choose or are required to use.

We hope that this initial technical note is the catalyst for productive feedback, discussion, and collaboration as we move toward a more effective means of managing for enterprise security.

Acknowledgements

Enterprise security management (ESM) is a concept that addresses and encompasses a broad range of security, management, and process-related topics, issues, and research areas. In an ESM approach, security is viewed as a collaborative effort that utilizes a broad array of organizational capabilities to be successful. In much the same way, our work in this area would not be possible without relying on the skills, knowledge, and insight found throughout the NSS Program. Over the past year, many members of this program (and the SEI) have unselfishly participated in countless conversations, discussions, and technical exchanges that have helped us to refine our thoughts and present them in this technical note.

Many NSS Program personnel deserve special mention for their contributions to the concepts included in this technical note. First and foremost, the author would like to thank the core members of the ESM team—Julia Allen, James Stevens, Bradford Willke, and William Wilson—who have provided a wealth of information and research to this project, and who have been willing to test our emerging concepts with the community.

We would also like to thank members of the CSIRT Development Team (especially Robin Ruefle) who have willingly allowed us to explore ESM concepts in the context of the process of incident management (which is surprisingly similar!). We extend thanks to Larry Rogers of the Practices, Development, and Training team, whose original drawings of a progressive approach to security have served to be a jumping-off point for our discussions and refinements of many ESM concepts. In addition, we thank Andy Moore and Carol Woody for their insightful review of the technical note. Last, but certainly not least, we would like to thank Rich Pethia for supporting this work, and for providing valuable guidance in shaping our research agenda and in providing practical application of this work to our customers.

We are also grateful to Pamela Curtis for her careful editing of this report and other enterprise security management work.

As always, we would also like to thank our sponsors for their support of this work. We believe it will have unprecedented impact on our customers' ability to refocus, redeploy, and vastly improve the ways in which they approach security in their organizations. It has already had great impact on our customers' ability to improve their security programs and on our ability to transition new technologies in the area of enterprise security management and enterprise resiliency.

Abstract

Security has become one of the most urgent issues for many organizations. It is an essential requirement for doing business in a globally networked economy and for achieving organizational goals and mission. But it is no small task. The technical and environmental complexity of today's organizations and the ever-increasing dependence on technology to drive and automate processes and create competitive advantages make security a challenging activity. Adding to this complexity is a growing list of vulnerabilities and increasingly sophisticated threats to which organizations are subjected on a daily basis.

Organizations can no longer be effective in managing security from the technical sidelines. Security lives in an organizational and operational context, and thus cannot be managed effectively as a stand-alone discipline. Because security is a business problem, the organization must activate, coordinate, deploy, and direct many of its existing core competencies to work together to provide effective solutions. And to sustain success, security at an enterprise level requires that the organization move toward a security management process that is strategic, systematic, and repeatable—in other words, efficient at using security resources and effective at meeting security goals on a consistent basis. Managing for enterprise security defines a disciplined and structured means for realizing these objectives.

This report presents the interim results of work done by members of the Networked Systems Survivability Program at the Software Engineering Institute in exploring these issues. The authors offer a view of the changing environment in which security must be performed and, from their field work and research, itemize characteristics of common existing approaches to security that limit effectiveness and success. A "desired state" as a security target for the organization is outlined, and the organizational transformation that the authors believe is essential for approaching security as a business problem is presented. Finally, the authors describe their current work in exploring solutions that they believe will enable this transformation.

1 Introduction

1.1 Background

Organizations face many challenges today in accomplishing their missions and in providing value to their stakeholders. What was once achievable by developing and implementing sound strategic and financial plans is no longer guaranteed. Instead, an organization must also consider how it is going to succeed in the face of increasing organizational and technical complexity and in an ever-changing risk environment. For organizations that aspire to be around in the next few years, adaptation and evolution are the mantras.

Success in meeting these challenges depends in large part on reducing the effects of complexity and change on the productivity of the organization. When unencumbered from interruption, an organization's critical assets and processes (those that most contribute to accomplishing the mission) can perform their intended functions and propel the organization toward achieving its goals, satisfying its critical success factors, and realizing its purpose and vision. Such is the emerging objective of security[1] in today's organizations: to enable the organization to thrive in a threat-rich environment.

1.2 The Emerging Role of Security

Organizations are being confronted with security incidents in record numbers. These incidents are not only more prevalent, but they represent a wide range of motives and intended consequences. For example, a scan of recent security articles and surveys describes events ranging from theft of information (such as customer credit card information) to "phishing" scams to wide-scale virus infections. And organizations are not just facing attacks that exploit technology. The terrorist attacks against the United States on September 11, 2001 used physical means to affect economic stability and interrupt the realization of economic, social, and political goals. The importance of these attacks is not that they target the organization's technical infrastructure or physical plant; instead, it is the interruption of the affected organization's quest to accomplish its mission that matters.

[1] The word "security" as used here is intended to describe the broad range of security activities that include the disciplines of information security, network security, application security, physical security, etc.

A technology-driven perspective on security obscures the fact that the productive elements[2] of the organization—people, assets, and processes—are the real focus of a protection strategy. For example, consider the use of a firewall device. A firewall places a technical barrier between the organization's network and the outside world. The intent of tweaking the firewall's rule sets isn't so much to protect the organization's network as it is to protect the business processes that rely on the network to accomplish the goals and objectives of the organization. From this perspective, the emerging role of security goes beyond simply protection to enabling productive elements to do their intended function. This gives the practice of security meaning because it takes into account the strategic drivers of the organization and evolves into a modern-day extension of the practice of risk management.

1.3 An Enterprise Approach to a Business Problem

Enterprise-wide issues that affect the organization's ability to accomplish its mission require organization-driven solutions. This lesson was learned in the Y2K crisis and it can be said of other enterprise-wide issues like diversity that require cultural changes and action on the part of all personnel. The quest for quality is another example. In the early 1980s, General Electric (GE) realized that their business model was insufficient for succeeding in a rapidly changing competitive environment. Most importantly, the model failed to focus on quality in customer interactions. GE's solution was to deploy a disciplined process for delivering high-quality products and services to customers called Six Sigma. The methodology they chose is not as important as the way they deployed it—working at every level of the organization, GE effectively inculcated a grass-roots movement toward quality, thus mobilizing everyone to solve an enterprise-wide problem. In effect, GE created a *culture* of quality that today describes how they work [GE 04].

Similar parallels can be drawn for security. The need to protect an organization's productive assets and processes *is a business problem* that can have disastrous effects on the organization's viability and resiliency if not addressed. Security strategies provide solutions for this problem. In turn, they also contribute to the viability and achievement of the organization's strategic drivers. As owners of critical assets and processes in the organization realize the value of security as an empowering function for ensuring goal achievement, a security-aware culture is seeded. Security becomes the way that the organization works, not something that it does.

1.4 Arriving at a New View of Security

Today's technology-centric view of security is misaligned with what drives the organization. This is often illustrated in the way that many organizations treat the role of chief security

[2] The term "productive elements" is used throughout this document to describe those elements that fundamentally contribute to the organization's achievements. While there is a compelling need to secure the safety of people, in terms of security, the focus is on critical assets (information, infrastructure) and processes.

officer (CSO). Once considered a promising recognition of the need to infuse a strategic element to security efforts, the CSO role is already reaching diminishing returns because of the failure of organizations to recognize the real purpose and intent of security. Some organizations simply do not know what to do with a CSO; some are eliminating the position or reducing what little authority CSOs had to act across the enterprise by pushing them further into the technical trenches of the organization or relegating them to little more than an overqualified security administrator [Berinato 04].

Recent experience and field work present abundant examples of the effects of a technology-driven perspective on security. At a minimum, it has resulted in failures of security efforts including misapplication of scarce security resources; ineffective security goal setting, measurement, and achievement; and misalignment between security goals and organizational drivers. Organizations are not setting meaningful security goals and are not able to know when and if they've reached the goals they do set.

In addition, these observations from our field work and research indicate continuing inability to move security much past a tactical activity performed at lower levels of the organization:

- the continued emphasis and focus on vulnerability analysis (identification and mitigation) as a primary security strategy
- an inability to leverage enterprise improvements in security from what is learned from information security risk assessments performed at operational levels of the organization
- failure to explicitly align security activities to strategic drivers using criteria such as an organization's critical success factors and to measure the achievement of security goals
- an inability to improve IT processes to the extent that they contribute significantly to reducing the organization's exposure to threats and vulnerabilities to key business processes
- relegation of security efforts to little more than a regulation-driven compliance activity
- failure of senior management to recognize the organizational value of security, to sponsor security efforts, and to recognize their role in security governance

2 Shifting Security Perspectives

There is compelling evidence that improvement in security requires changing old perceptions and defining new targets. The evolution of security as a practice is highly dependent on providing approaches and solutions that take into consideration the dynamic, complex, distributed organization that is the canvas for today's CSO. Clearly, the days of security generating from the IT department and being controlled and managed from an IT vantage point are beginning to fade. Instead, security must be repositioned as the byproduct of wider ranging efforts that aim to make the organization more resilient to its ever-changing risk environment. Today, organizations ignore their risk tolerances and the enterprise-wide consequences of their inaction to their own peril.

2.1 Drivers for Change[3]

In our field work and research, we have identified two notions that are forcing changes in the way that organizations approach security: the unbounded organization and the pervasiveness of technology. Today's organizations are like cells in that they are inextricably connected to their surrounding environment. More and more, organizations are forced to provide access to traditional "outsiders" such as vendors and business partners to their most critical organizational assets as though they were insiders. The popularity of ERP-type systems to manage supply chains is evidence of this as well as the increase in outsourcing of horizontal business processes such as payroll, accounts receivable and payable, and even IT management. Economic drivers are forcing some of these changes, but the organization's need to rely on its outside environment to accomplish its mission is more prevalent than ever.

The unbounded organization is being enabled and fueled by technology. The Internet has single-handedly created permeable borders for organizations. But the technology influence doesn't end there. Organizations are adopting technology at escalating rates because it enables them to achieve their goals more effectively and efficiently and accomplish their mission. Technology also often brings competitive advantages. Consider the effect of technology on retailing—transactions are paperless and moneyless; supplier automation makes the supplier a virtual insider to the organization so that the product life cycle is integrated across development and delivery. The overall effect has been falling prices for consumers and (unfortunately) an elimination of competition by organizations that have failed to automate to this degree.

[3] Our initial thoughts on the drivers for changes in the way that security is approached and managed can be found in a white paper entitled "The Challenges of Security Management" [Caralli 04a].

The weaving of technology into virtually all of the organization's critical business processes brings a level of complexity that is difficult to support and that exposes these business processes to interruption. More connections to the outside environment bring an increasingly rich source of vulnerabilities, threats, and risks that the organization must confront and adapt to.

All of this is fodder for characterizing the challenges that organizations are facing as they address the protection needs of their assets and processes and apply security in an effective and efficient way. In this section, we offer our characterization of the way that security is perceived by many organizations today. Then we provide a view of where we believe the practice of security will evolve.[4]

2.2 Characterizing the Challenges

Security lives in an organizational and operational context, not as an isolated discipline. Effective security must take into account the dynamically changing risk environment within which most organizations are expected to survive and thrive. To achieve and sustain an adequate level of security that directly supports the mission of the organization, senior management must shift their point of view (or frame of reference) and that of their organization from an information-technology-based, security-centric, technology-solution perspective to an enterprise-based, risk management, organizational continuity and resilience perspective. This requires moving well beyond ad hoc, reactive approaches to security (lacking process and procedure, and dependent on individual heroics) to approaches that are process-centered, strategic, and adaptive. The CSO must be able to draw on the capabilities of the entire organization so that they can be deployed to address a problem requiring an enterprise-wide solution set. However, because security isn't a one shot activity, it also means being able to achieve it in a way that is sustainable—systematic, documented, repeatable, optimized, and adequate with respect to the organization's strategic drivers.[5]

2.3 Shifting Security Perspectives

There are six shifts in perspective or thinking that we believe are essential to characterizing the practice and management of security from a technology-solution point of view to one that is guided and influenced by enterprise-wide concerns. Table 1 summarizes these shifts, followed by detailed discussions on each area.

[4] Earlier work in characterizing shifting security perspectives (toward the notion of survivability) can be found in "Information Survivability: Required Shifts in Perspective" [Allen 02].

[5] Throughout this document, the term "strategic drivers" refers collectively to the organization's mission, goals, objectives, and critical success factors—everything necessary to ensure that the organization achieves its value and purpose. In some cases, we also use the term "organizational drivers" similarly.

Table 1: Shifting Security Perspectives

Area	Shifting From	Shifting To
Security scope	Technical	Organizational
Ownership of security	Information technology	Organization
Focus of security	Discontinuous and intermittent	Integrated
Funding for security	Expense	Investment
Security drivers	External	Internal
Security approach	Ad hoc	Managed

2.3.1 Scope: Technical to Organizational

One of the first questions that an organization must consider with respect to security is, What is the scope and extent of security concern within the organization?

Today, it is clear that most organizations focus security activities on their IT-maintained system and network infrastructure. Technology-based solutions (such as running antivirus software, protecting the network perimeter, configuring firewalls properly, and installing host-based intrusion detection) define the *primary* security activities that are performed. And the focus is on technical assets (desktops, laptops, servers, databases, remote devices) in lieu of information and other organizational assets. As a result, security is considered to be a technical specialty where the knowledge, skills, and capabilities are owned by IT staff and system administrators.

In addition to minimizing coverage of the enterprise, a focus on the technical infrastructure of the organization obscures the value of organizational assets such as information. Technical assets have value because they store, transport, and process *information* assets and support business processes and services. Thus, if the organization is misled into placing higher value on the technical assets, protection strategies often do not consider the value of the underlying assets and processes. Organizations that take a technical focus fail to consider that risks to the technical infrastructure are important because they also threaten the confidentiality, integrity, or availability of information assets or they disrupt or disable the organization's business processes. A technical focus also limits the organization's ability to ensure protection of information assets that are not dependent on or connected to the organization's technical infrastructure. For example, an organization may store its product designs on paper or keep its medical records in paper form—both of which may be critical for meeting the organization's mission. Securing the organization's technical infrastructure alone does not provide a proper level of protection for these assets. Thus, when an organization takes a pulse regarding their security effectiveness by only considering the state of their technical assets, they are potentially lulled into a false sense of security.

Effective security management requires a considerably broadened scope. The organization needs to be the catalyst for setting and prioritizing security requirements that align with business objectives. Under an *organizational model*, the focus of security shifts from the "technical network" to the "organizational network" that comprises people, processes, business units, and relationships with customers, partners, and suppliers. Organizational assets are information-centric (customer data, employee data, sensitive communications, critical business processes) and their protection is the primary security concern. Meeting organizational requirements such as protecting customer privacy and ensuring authorized access to information becomes the driver for security priorities.

In organizations that have accomplished this shift, security management is accepted and rewarded as an organizational competency, even if some of the security services are provided by outside parties. In this model, security is so inextricably tied to the success of the organization in accomplishing its mission and improving its resiliency that it is in the organization's best interest to be competent at securing itself.

2.3.2 Ownership: IT to Organizational

Who owns the security issue in an organization? Who should be held accountable for it?

Ownership addresses who has the authority, accountability, and responsibility to act when it comes to security, and who owns the security concern. In many organizations, IT is viewed as the driver, owner, and benefactor of security. Security is relegated to a technical concern and the organization's strategic drivers are ignored.

The organization is the ultimate benefactor of investments in security. Thus the organization, not IT, needs to set security priorities, drive security actions, and own the security strategy. Business unit and department managers have a stake in and must be held responsible for the protection of the assets (information and otherwise) and processes that they own. CSOs cannot be effective unless they are able to direct and control resources at the organizational level, serving as a trusted advisor to the organization instead of a technical advisor running interference on the latest security incident or deployment of the latest security product, service, or patch. And boards of directors and senior leadership must be the governing factors for security in much the same way that they govern over other business initiatives and issues.

2.3.3 Focus: Discontinuous to Integrated

How does an organization apply security—waiting and responding to events, or as a strategic, continuous process that is part of doing business?

An organization's attention typically turns to security in response to a damaging attack such as a new virus or worm. In this way, security is specifically focused on an event. Over time, this leads to a discontinuous security approach. The practice of security becomes intermittent and tactical and is isolated from other aspects of conducting business in the organization. As a result, the organization fails to cultivate a security culture and finds long-term success in stabilizing its environment unachievable.

Discontinuity often is instigated by an organization's response to new regulatory requirements, causing yet another flurry of activity that dissipates over time, is focused on the wrong organizational drivers,[6] and fails to provide any organizational learning. Eventually, the organization experiences diminishing returns with respect to its security investments. As an organization continues to manage security in discrete, event-driven fragments, the resources they use are not necessarily focused on long-term value for the organization. At some point, this approach becomes disjointed and does not produce desired results, and resources (money, technology, and people) are depleted. The failure to manage security to the strategic drivers of the organization results in a whole that does not equal the sum of its parts.

To be successful in the long run, organizations must integrate their approach to security into the day-to-day management of their business processes in order to avoid diminishing returns. Security becomes a consideration in normal planning cycles and major decisions (such as system development projects). Organizations use their regular risk management process to determine what parts of the organization to focus on so that their security investments provide long-term value. Addressing security events does not require the organization to do additional activities or go outside of their normal business processes. And security controls that the organization implements meet regulatory and audit compliance requirements or are seamlessly updated to do so with minimal disruption to ongoing processes. Eventually, security becomes routine—it's difficult at first, but later it becomes second nature, invisible, and transparent. In fact, directly focusing on it produces less-than-optimal results.

2.3.4 Funding: Expense to Investment

How do organizations pay for security? And how do they know if investing in security has produced the desired benefit, including a positive return?

Traditionally, organizations view security as an expense—an expense that is often hard to justify because it only has meaning in the context of a risk that hasn't yet been realized. As an expense, it negatively affects the organization's bottom line by eating into the organization's profits and becoming a sunk cost that the organization cannot recover. Worse yet, the benefits derived from this cost are difficult if not impossible to measure—they are often realized only after an incident has occurred. Organizations are also faced with the problem of prioritizing

[6] For example, organizations often contact us for help as the result of a regulatory deadline that they need to meet. While this is a good catalyst for action, it generally ends up shaping and defining an organization's security strategy by default. When this happens, the security strategy is aligned with compliance to regulations, not the organization's strategic drivers. It is easy to imagine that there are some cases in which failing to comply with regulations actually is in the best interest of the organization.

security costs—which are more important: technical controls, monitoring software, security staff, or CSOs? Organizations have no incentive to characterize security costs in any other way—there are no widely accepted standards and measures against which to benchmark security investments, and there is no competitive demand to demonstrate an acceptable level of security capability.

Properly positioned, security supports the productivity of the organization's people, critical assets, and processes. From this perspective, security is an investment in the productivity of the organization toward accomplishing its mission. When the organization views security as an investment, it is more likely to demand projected benefits in advance (as for other business investments) and to regularly collect and report meaningful metrics that can be used to evaluate security performance. In this view, the return on security investment is measured, quantifiable, and thus demonstrated. Such information can be used in prioritizing and valuing security activities.

An organization that successfully approaches security as an investment may also increase its overall value in the marketplace, as is often demonstrated by the concept of "goodwill."[7] In fact, in the future, a determinant of an organization's value may be the amount of goodwill it can provide to acquiring companies that is directly due to its ability to secure critical assets and processes and improve its resiliency. Certainly, an organization that can keep its core assets and processes in service in the face of an attack, accident, or failure (and actually improve their ability to adapt to future events) may be worth more than one that cannot, if only because of the competitive advantage they create.

Security as an investment in the organization's long-term viability and resiliency gives security activities purpose and value. In organizations that achieve this shift, security goals are specific, measurable, tangible, and part of regular status reporting and business planning—supporting the assertion that security can, at a minimum, preserve an organization's bottom line, if not improve it.

2.3.5 Security Drivers: External to Internal

What drives the security actions of the organization? What provides the impetus to act?

There is an increasing proliferation of recommended security standards, guidelines, regulations, checklists, surveys, and case studies. How does an organization decide what security practices to implement?

While such sources can help an organization in selecting and implementing security practices, they are not a good substitute for a security strategy that is forged from and

[7] For accounting purposes, goodwill is an intangible asset valued according to the advantage or reputation a business has acquired over and above its tangible assets. Any factor that translates into the organization's ability to increase its earning power (or ability to accomplish its mission) can contribute to goodwill, such as its reputation, customer service, and perhaps its ability to adapt to changing risk environments.

executed based on the organization's strategic drivers. When organizations use externally produced best practices (even though they may be provided by a trusted and reputable source) or use the need to comply with regulations as their primary security driver, there is a good chance that they will either oversecure or undersecure their critical assets and processes, thus directing their limited security resources inefficiently.

Security practices must be implemented in the organization's context; what works in one organization may not work in another because they have different drivers and, more importantly, risk tolerances.[8] Above all, the focus should be on developing a top-down strategy for security that permits the integration of many different types and sources of security practices and provides for compliance with the relevant regulations for the organization. Indeed, it is a rare organization that is subject to comply with only one regulatory body. Thus, organizations have an advantage where they seek first to manage the security process to the organization's drivers and second to pick and choose the appropriate security practices to support it. Compliance becomes a byproduct of a sound security strategy, and organizations achieve a level of adequate security that is commensurate with their strategic drivers, not "absolute" in the sense of trying to comply with all possible regulations and implement all best practices available.

2.3.6 Approach: Ad Hoc to Managed

How does an organization manage security? What capabilities do they employ?

Many organizations do not have a strategic view of security and consequently do not have a true security strategy. They consider security only when forced to (in the face of an attack) or when the next wave of technical solutions comes along, resulting in an approach that relies on tactical, reactive, improvised activities dependent on individual skills and heroics.[9] Requirements for security and the commensurate response are developed as events or attacks occur, monitoring what has happened and often taking action after the fact. The notion of security as solely necessary for protection or defense evolves from this more reactive approach. As organizational and technical complexity increases and the risk environment changes, the organization struggles to keep up.

Organizations are better served by viewing security in a deliberate, systematic, and strategic manner that enables the accomplishment of their mission. From this position, security is viewed as enabling information-dependent business processes and as a means for adapting (versus reacting) to complexity and more easily accommodating a dynamically changing risk environment. Security policies, procedures, and processes are planned, repeatable, and sustainable. Security is viewed proactively with processes and technology in place that sense

[8] In fact, there may be other drivers that make an organization unique and upon which security practice selection should be based: competitive drivers, market position, financial position and condition, risk, etc.

[9] Not unlike a common issue in organizations that lack mature processes for developing software.

the risk and threat environment in advance of events occurring, to the extent possible. Staff members are recognized and rewarded for consistency, discipline, and their ability to predictably execute, measure, and improve defined processes.[10]

Depending on the security target that they are trying to achieve and sustain, organizations may employ a wide range of approaches to security management that embody the upper and lower limits of these shifts in perspective. A range of common approaches to security management that characterize this from our purview are presented in Section 4, "Four Notional Approaches to Security Management."

For reference, Appendix A also provides an expanded summary of these shifting security perspectives.

2.4 Shifting Toward Organizational Resiliency

One of the most important questions an organization can ask is, What is the goal of our security efforts?

As security begins to demand more of an organization's financial resources, the organization must ask why an investment in security is justified. Organizations are full of anecdotal evidence of security's importance, but they are hard-pressed to articulate the actual benefits they've received or the goals that they are trying to achieve. Consider the organization that has an event-driven approach to security—instead of deploying a security strategy that works toward achieving organizational goals, the goal is to "solve" each security incident or event. An organization can fill a room with the results of a network vulnerability scan, but experience tells us that only some of the exposures really matter to the organization and should be given attention. In fact, it may not be in the best interest of the organization to care about the next virus infection or the latest publicized vulnerability, yet resources are applied to these activities usually without much hesitation. Organizations that view security in this way also tend to aim toward an "absolute" articulation of security; that is, they try to secure everything they can to the extent possible without considering the level of protection that is balanced between need and cost.

An outcome of this approach to security is the failure to define and work toward a desired security target—one that meets the security requirements of the organization and is balanced with risk and competing needs for constrained organizational resources. Security must contribute to improving the organization's ability to withstand potentially disruptive events and to adapt to dynamically changing risk and threat environments—in other words, looking beyond security to improving and sustaining the organization's resiliency as the primary goal.

[10] There is much to learn from the software process improvement community in this area. This approach to organizational capability or maturity for security management draws heavily on these lessons.

2.4.1 Resiliency Explained

Resiliency is an emerging concept for security. In the material sciences world, it is commonly known as the property of a material (such as steel or aluminum) to be altered in some way and to regain its original shape after altering forces have relented. Resiliency in an organizational context is similar. *Organizational resiliency* describes the organization's ability to stretch beyond its natural limits when necessary and to be able to return to its normal operating state. It defines the adeptness of the organization to withstand systemic discontinuities and adapt to changing risk environments [Booz 04]. Equally important, it also defines the organization's ability to be *prepared* to adapt before operational and environmental circumstances force it to do so [Hamel 03].

2.4.2 Resiliency, Risk, and Security

Risk and the practice of security are essential components of organizational resiliency. Risk management is a primary function of all organizations, whether it is done explicitly (i.e., there is a chief risk officer), implicitly (as part of the decisions that each manager makes on a daily basis), or both. A risk management approach to security is a step toward aligning security with strategic drivers. When an organization aims to improve or sustain its resiliency, it must take appropriate enterprise-wide actions such as aligning its strategy, operations, systems, governance structure, and other capabilities so that it can uncover and adjust to risk in a transparent (i.e., systematic and controlled) manner [Booz 04]. The ability of an organization to adapt to a changing risk environment affects its organizational resiliency—failing to adapt to a changing risk environment lowers the organization's resiliency.

As an extension of risk management, the practice of security is aimed at protecting the organization's productive elements from being impeded, disrupted, or destroyed. The resistance of these productive elements to attack, intrusion, or other events improves the organization's resiliency. An organization that exhibits high resiliency is not affected by disruptions to these elements and in fact may be fortified against future disruptions as a result; on the contrary, a less resilient organization suffers productivity losses and in the most extreme cases, never recovers.

2.4.3 Organizational Resiliency as a Goal of Security

When an organization secures its productive elements, it ensures that their contribution to the mission continues unabated. Thus, the practice of security can be redefined as the actions the organization takes to enable its productive elements with the higher purpose of improving or sustaining the organization's resiliency. In this context, the practice of security becomes a contributor to the organization's ability to adapt to new risk environments and minimize disruptions, and a better target for the improvement and maturity of an organization's security strategies and processes is provided.

2.4.4 Organizational Resiliency and Transparent Security

Above all, resilient organizations establish transparency [Booz 04]. Transparency describes the ability of the organization to perform risk adaptation and management in a way that is assimilated into the operational culture and structure of the organization. In other words, resiliency (and by default, security) is how the organization operates. Eventually, the organization migrates away from traditional security practices because the management of productive elements is expanded to provide for their long-term viability. In transparency, the organization's productive elements, including business processes, become self-healing—each element is managed with an eye toward resiliency so that there is no impact to its productivity in the event of an intrusion or other discontinuity.

2.5 Summary

Security needs to be positioned as an enabler of the organization—it must take its place alongside human resources, financial resources, sound business processes and strategies, information technology, and intellectual capital as the elements of success for accomplishing the mission. As organizations expand their view and perspective of security, they also elevate the purpose and goal of security and position it as an essential success factor for the organization.

Effectively directed security activities and strategies contribute to the quest for organizational resiliency. Achievement of improved and sustainable organizational resiliency provides the "carrot" that organizations need to catalyze their movement away from security as a technology-centric activity to one that positions security as an essential contributor to the organization's strategic drivers.

3 Advancing the Management of Security

The challenge for organizations is to advance their security efforts to a higher level of organizational alignment; to take an enterprise view and manage security from an enterprise perspective. While it is certainly too early to provide a comprehensive approach to security improvement, our research and field work are yielding compelling elements of a solution to the challenges that organizations are currently facing. This section provides our view of the foundational principles of managing for enterprise security.

3.1 Defining Enterprise Security Management

From a process perspective, management can be viewed as the ability to actively control a process so that it performs as specified and reaches its goals and mission. When applied in the context of "enterprise security management," the word "management" is intended to impart the need for active planning, controlling, and coordination of activities across an enterprise so that security goals can be reached. In essence, managing security[11] is planning, organizing, commanding, coordinating, and controlling it for the benefit of all stakeholders; in other words, managing for enterprise security is an essential organizational process.

3.2 Foundational Principles of ESM

Our work has resulted in the identification of several essential principles that characterize an enterprise management approach to security. These principles are as follows:

- Align with strategic drivers.
- Provide sponsorship and governance.
- Focus on productive elements – assets and processes.
- Define the security target.
- Sustain the system of internal controls.
- Manage and improve IT services and operations.
- Target the entire asset life cycle.
- Measure goal achievement.
- Utilize core capabilities.

[11] Management essentially means "the act, manner, or practice of managing; handling, supervision, or control." At the turn of the 20th century, Henri Fayol essentially codified this definition into his five activities or functions of managers: planning, organizing, commanding, coordinating (activities), and controlling (performance).

Each of these concepts is described in more detail below.

3.2.1 Align with Strategic Drivers

An enterprise approach to security—one that makes security a core competency of the organization—must be motivated by the same drivers that propel the organization toward its mission. Misalignment between security activities and an organization's strategic drivers is a primary reason why many organizations do not realize substantial improvements in security even though they are assigning significantly larger amounts of resources to it. In effect, because the resources are not aimed at achieving the organization's strategic drivers, they also do not significantly improve the organization's resiliency.

This is particularly evident in organizations that take a technology-centric view of security. Many organizations acquire and implement cutting-edge security technologies yet cannot report significant improvements in realizing security goals. Our field work has witnessed this time and time again—a new firewall device is implemented, but the firewall rules are set by the IT department, which fails to account for the security requirements even of users who use the network that the firewall is intended to protect. Or consider the increase in risk assessment activity in organizations. Many organizations still believe that organizational risk assessment should be performed by IT personnel because *they* have the responsibility for security. This has been a particularly frustrating observation in our work with the CERT® Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®) method—students who attend OCTAVE training are often IT personnel who cannot make decisions about the security needs of important assets in their organizations, rather than the business personnel who own those assets.

Corporate culture is also a huge contributor to misalignment. The attitude of senior executives that security is a technical issue and that the CSO is a technical resource is fueling the misalignment between security and strategic drivers. Unlike the progression of the role of chief information officer (CIO), chief security officers still find themselves looking into strategic planning activities, rather than being a part of them [Berinato 04].

3.2.2 Provide Sponsorship and Governance

In many of the SEI's software engineering improvement initiatives, executive awareness, understanding, and education have been found to be essential to initiate, achieve, and sustain any level of improvement such that it becomes part of normal business conduct. This concept was instantiated in the use of the SEI IDEAL℠ model for organizational improvement as the "initiating" phase—setting context, building sponsorship, and developing a charter infrastructure for improvement [Gremba 97]. Executive sponsorship is also a foundational

® CERT and OCTAVE are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

℠ Operationally Critical Threat, Asset, and Vulnerability Evaluation and IDEAL are service marks of Carnegie Mellon University.

element in process improvement techniques such as Six Sigma. An organization's ability to mobilize to achieve and, more importantly, to sustain a desired security state starts with executive sponsorship, enacted and sustained by governance. Those who lead, manage, set strategy, and are held accountable for an organization's success set the direction for how enterprise security is perceived, prioritized, managed, and implemented. If the responsibility for enterprise security is relegated to a role in the organization that lacks the authority, accountability, and resources to act and enforce, the organization's security state will mirror this [Allen 04].

3.2.3 Focus on Productive Elements

The principle of "focus on the critical few" is a fundamental element of risk management [Alberts 01]. It is also an essential element of a strategic approach to security because the organization does not have unlimited resources with which to identify and mitigate all risks. Thus, as is reinforced throughout this report, the focus of the practice of security must be on the critical assets and processes of the organization—those productive elements that most contribute to the organization's success.

3.2.3.1 Processes

Processes describe the systematic ways in which organizations accomplish work. Every activity in an organization can be associated with one or more processes. A process has a mission that is tied to the overall mission of the organization; critical processes are those whose mission is vitally important to the achievement of the organization's mission.[12] An enterprise view of security focuses on processes because their disruption has the potential to impact the organization.

3.2.3.2 Assets

Assets define the things that are of value to the organization. In the broadest sense, they can include people, information and data, physical plant, and other tangible and intangible items of value such as property rights and goodwill. The assets that are of most importance in an enterprise security management view are those that are needed by critical processes that the organization performs in order to accomplish its mission.[13] Most often, these are information assets and infrastructure assets that support processes.

[12] Efficiency studies and process reengineering efforts often uncover inefficient or non-critical processes and position them as candidates for elimination, along with associated assets and, unfortunately, personnel. This is generally based on an implicit valuation of the process's value and contribution to accomplishing the organization's mission.

[13] For simplicity, we notionally focus on information assets and infrastructure assets (such as workstations, servers, networks) that support automated processes. We realize, however, that information assets may exist in many different forms (such as paper or in databases) and that not all processes in the organization are automated (and therefore are not reliant on infrastructure to operate). In addition, when the organization broadens its view to resiliency, it must consider a wider range of assets such as physical property (fleet, office furniture) and physical plant (buildings, land)

3.2.4 Define the Security Target

Surely, one of the most imposing obstacles to an organization's security efforts is being able to describe what success looks like. In the absence of affirmative data, many organizations resort to describing success as the absence of a security incident, event, or even a vulnerability.[14] In addition, some see security as an endstate—something they will achieve and then maintain—rather than a continuous effort that is subject to the same pressures and influences as the organization.

In simple terms, the organization's security target is the satisfaction of the security requirements of the organization's critical assets and processes. In reality, an organization's security target is more complex and has several dimensions that must be considered.

1. The security target is a factor of an organization's unique strategic drivers and mission. For example, the security target of a government contractor that works with sensitive Department of Defense information and systems is different from that of a county government.
2. An organization's security target is not static—as the organization's risk environment changes and it is exposed to varying levels of complexity (organizational, technical, etc.), its security requirements change. As security requirements change, so does the organization's security goals and objectives. This constantly changing target means that security is never "reached" and requires security strategies to be flexible, dynamic, and continually improving.
3. The security target is a point of equilibrium for the organization—an appropriate balance between security efforts, security requirements, and risk. This equilibrium describes a level of "adequate security"—no more and no less than is required to keep the organization's critical assets and processes functioning as intended to meet the organization's mission within acceptable risk tolerances.[15] Actions that go beyond

that it needs to operate and to accomplish its mission. From a security management perspective, these assets are important if they are impacted (i.e., can't perform their mission) by failure to properly secure a critical asset or process that uses information and infrastructure assets.

[14] Some organizations that we have observed believe that the lack of exposure to common vulnerabilities is an indication of the success of their security programs. But what they fail to realize is that they are only measuring success against *known* vulnerabilities, not those that could potentially affect them and have yet to be discovered. In addition, this approach considers only vulnerabilities that arise in technology, not the organization as a whole. This is a reason why a vulnerability-driven approach is often incomplete.

[15] This is in stark contrast to "absolute security." Organizations that apply security controls without regard to the organization's strategic drivers are at risk for not only protecting the wrong assets and processes (i.e., those that are not necessarily important to the mission), but potentially over-protecting critical assets and processes simply because the technology exists and is affordable. A good example is when organizations implement a public key infrastructure for authentication when a lesser technique might provide the appropriate (and most cost-effective) level of protection. Not only can an "absolute security" attitude result in over-protection, it can also constrain assets and processes from doing their job. After all, one way to solve the security issue in an organization is to lock everything down; unfortunately, no one would be able to do their job and the organization would never achieve its goals.

"adequate security" essentially result in protection costs that exceed the risks to and value of the assets and processes they protect.

In the context of managing for enterprise security, we notionally refer to the security target as the "secure state" of an organization. While there is certainly more work needed to define and codify the concept of a secure state, it is nonetheless a cornerstone of improving an organization's security efforts (not unlike similar concepts found in quality and process improvement). Thus, an essential part of our work in enterprise security management focuses on enabling an organization to systematically, consistently, and tangibly define its secure state in a way that allows it to measure the success of its security efforts and continually improve them.

3.2.5 Sustain the System of Internal Controls[16]

Auditors have long known that the mission of an organization is most at risk when an appropriate level of internal controls has not been implemented or when the controls that have been implemented are circumvented or prevented from operating properly. This is the primary reason why auditors perform internal control reviews—exposures in the system of internal controls are potential risks to the organization.

In an enterprise view of security, the ability to reach and sustain a secure state is highly dependent on proper installation and operation of the organization's system of internal controls. These controls are implemented to ensure that processes are accomplishing their mission within a level of variation that is commensurate with the organization's risk tolerance. When a process is operating properly, its contribution to the overall mission is ensured and, more importantly, there is additional assurance that the process does not become a source of risk for the organization. For example, consider the process for paying vendors. A lack of controls in this process[17] could result in duplicate payments (i.e., a vendor being paid for the same invoice more than once), overpayments (i.e., a vendor being paid more than the charges on the invoice), or late payments. At a minimum, these variations in the payment process result in financial exposures to the organization. At worst, late payments could result in vendors refusing to continue supplying raw materials, products, etc., which would eventually cause discontinuities in the organization's supply chain, thereby reducing the overall resiliency of the organization.

If the underlying motivation for the security activities in an organization is to ensure its resiliency, it must consider the effect of the system of internal controls in addition to meeting the security requirements of the organization's critical assets. Indeed, control-based practices such as CobiT[18] and ITIL,[19] which are mostly aimed at IT service delivery and operations,

[16] The "system of internal controls" is a commonly used auditing reference to the controls placed throughout the processes of the organization to control variability and ensure protection from exposures such as fraud.

[17] A lack of controls could mean either that the controls do not exist or that the existing controls do not work properly, resulting in a variation of the process from expected results.

[18] See Section 5.2.2.

[19] See Section 5.2.3.

recognize these broader objectives of security. True resiliency for an organization means that it can withstand all types of discontinuities, mostly because it has established a proper level of internal controls and because it has aligned its core capabilities so that it can adapt to risk without disruptive or disabling impact [Booz 04].

3.2.6 Manage and Improve IT Services and Operations

Information technology abounds in today's organizations. The organization's business processes are increasingly being automated, and if the organization wants to compete and thrive, it must be willing to connect to operational and technical networks both inside and outside of its boundaries. This reliance on technology results in an expanding, dynamic infrastructure that can prove to be a never-ending source of vulnerabilities, threats, and risks to the organization.

Fortunately, from a security and resiliency perspective, there is a silver lining in this pervasive use of technology: there is mounting and compelling evidence that organizations that achieve improved levels of control in delivering IT services and managing IT operations also reap benefits in reducing their exposure to vulnerabilities and discontinuities that affect organizations.[20] Indeed, the SEI has spent considerable energy studying this connection. The CERT Coordination Center® has long advised that regular patching of systems with up-to-date software releases alone reduces an organization's exposure to known vulnerabilities. More recently, the SEI began collaborations with outside organizations and convened a group of high-performing[21] organizations that have been achieving improved levels of security through an IT operations perspective.[22] Results of information benchmarking indicate that these organizations create [Behr 04][23]

- higher service levels
- a high percentage of planned, scheduled work
- unusually efficient cost structures

[20] Security is not the specific goal of these activities, but is the indirect result. Thus, another case is made for aiming at a higher purpose such as IT operations and service delivery excellence and obtaining security as a byproduct.

® CERT Coordination Center is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

[21] Our working definition of a high-performing security and IT organization is one that successfully applies resources to accomplish stated objectives, evolves a system of process improvement as a natural result of its business demands, and regularly implements repeatable, predictable, definable, secure, and measurable operational processes (Allen, Julia et al., "Best in Class Security and Operations Roundtable Report," Carnegie Mellon University, Software Engineering Institute, February 2004; available upon request).

[22] Specifically, this work concentrates on considering patch management in the context of broader change management (Taylor, Jay; Allen, Julia; Hyatt, Glenn; & Kim, Gene, "Change and Patch Management: Critical for Organizational Success," Global Technology Audit Guide Series, Institute of Internal Auditors, March 2005; available upon request).

[23] Allen, Julia et al., "Best in Class Security and Operations Roundtable Report," Carnegie Mellon University, Software Engineering Institute, February 2004.

- a high percentage of time spent in proactive mode
- productive working relationships with peers
- fewest security incidents
- earliest integration of information security requirements in the service delivery life cycle
- an ability to devote increasingly more time and resources to strategic issues, having mastered tactical concerns

These organizations also attempt to measure their successes where possible.

In the most simple sense, being effective at IT service delivery and operations tends to reduce an organization's exposure, at least from a technical standpoint. Since this area of the organization often provides a large portion of its risk environment, controlling services and operations can significantly cut down the enterprise's exposure as well.

3.2.7 Target the Entire Asset Life Cycle[24]

One of the reasons that organizations tend toward a reactive approach to security management is because they do not address threats and vulnerabilities to their technical assets until they are in the operation and maintenance phase of their life cycle. Assets in this phase are relied on by the organization because they automate or support key business processes. Threats to these assets become potential discontinuities to the organization, forcing the organization to respond. Frequently, this means redeploying resources from other important tasks and an overall increase in costs to the organization. For example, consider a key organizational application system such as a production control system. If it is threatened or attacked, the organization incurs costs related to

- finding and fixing the vulnerability that was exploited,
- implementing business continuity plans and programs to ensure continuity of the production process while the system is being repaired, and
- managing consequences, which could include production downtime, missed customer orders, affects on reputation, potential lawsuits, etc.

New and emerging vulnerabilities continue to threaten operational assets. However, many threats and vulnerabilities manifest themselves in the operations phase of the asset's life cycle only because they have not been addressed earlier in the asset's planning, analysis, and design. This is particularly true when organizations acquire software and systems—they bring into the organization many of the vulnerabilities that the vendor may have inadvertently "built into" the system.

An enterprise view of security requires the organization to actively reduce an asset's range of vulnerabilities as well as to actively manage the potential impacts to the organization if an

[24] The life cycle is described simply as the planning, analysis, design, implementation, and operation phases. For an application system, this life cycle closely parallels the traditional systems development phases.

asset is compromised. This is done by addressing vulnerabilities at the earliest point of origin, which is more cost and resource effective than doing so when an asset is in operation. For software development, this means actively engineering-in controls and engineering-out potential defects that can affect the asset in operation.[25] For business processes that are automated, this means implementing preventative and deterrent controls early in the process flow so that more costly and less effective corrective, compensating, and detective controls do not have to be used in the operations phase, particularly when they require human intervention. Approaches to security management that do not promote this "earlier is better" means for reducing variability ultimately reduce the organization's resiliency.

3.2.8 Measure Goal Achievement

The view of security as overhead is an unfortunate outgrowth of the lack of inclusion of measurement and metrics as an essential element of security management. Organizations do not routinely require return on investment (ROI) calculations on security investments, nor do they attempt to measure or gather metrics on the performance of security investments. Absent a set of established and accepted metrics for measuring security ROI,[26] there is little an organization can do other than perform measurement in the context of incident avoidance (which it may never know) or the impact of a realized risk (i.e., the control costs less than the consequence, and therefore provides a positive return).

Measuring the effectiveness of the organization's security activities is essential to determining whether they ultimately contribute to attaining and sustaining the organization's secure state and improving resiliency. But measurement is also important because it allows the organization to more confidently state realized benefits from security efforts and because it moves the organization toward an investment-focused view of security.

Measurement is at the center of process improvement. Enterprise security management can be viewed as a metaprocess that requires measurement to ensure goal achievement. As with any process, variability in enterprise security management can take the organization outside of its risk tolerances and consequently reduce its resiliency. In the long run, failure to measure the effectiveness of enterprise security management impedes the organization's ability to improve and optimize security as it adapts to changing risk environments.

[25] Indeed, deploying patches for software, hardware, and systems often results from the need to eliminate or reduce exposure due to weaknesses that could be exploited. These weaknesses often could have been prevented by implementing good software engineering practices so that fixes do not have to be implemented in the operations phase, where they are more costly and disruptive.

[26] Measuring security return on investment is necessary to ensure that scarce security resources are being focused on the right assets and processes—those that are necessary to accomplish the organization's mission. Thinking of security in terms of ROI is one way to elevate security to the level of other business processes that senior managers are responsible for managing.

3.2.9 Utilize Core Capabilities

The enterprise security management concept asserts that there is a core set of operational and managerial capabilities that an organization must possess to be able to carry out its security goals and objectives. In many cases, these are the same capabilities that the organization needs to achieve its mission, albeit expanded to include security in their scope. Field work and research thus far show that these capabilities

- do not always include security as their primary area of focus
- represent many of the core (horizontal) competencies that organizations already have and need to conduct business
- are usually necessary for organizations to achieve their critical success factors and accomplish their missions
- are executed throughout the organization and are not concentrated in any one operational unit or department
- are both strategic and tactical in nature

When performance of these capabilities has been optimized, and when the capabilities are coordinated to work together for common security goals and objectives, organizations tend to be "doing security" even though the security activities are transparent and not explicit.

Early work performed with high-performing organizations confirms some of these notions. For example, some of these organizations reported security improvements through optimization of core IT service and operations capabilities. Indeed, it is easy to see that practices prescribed in methodologies such as CobiT and ITIL have IT process improvement at their core but easily translate to potential improvements in security and resiliency. Consider an organization's configuration and change management capabilities—if performed consistently with high quality, many of the vulnerabilities that organizations like CERT report on a daily basis become less of a potential threat because software updates are regularly installed. Or consider an effective release management capability—an organization that does this well can reap benefits from being able to predictably control what goes into the organization's production environment.

There is promise for expanding this concept to utilize other organizational and operational capabilities in achieving security goals. For example, consider a function such as asset management—an organization that formally controls the identification, description, and inventorying of its critical assets improves its ability to focus its security resources because it has a clearer vision of what assets need to be protected, why they are important to the organization (in accomplishing its mission), and how the organization would be impacted if they were compromised.

3.3 Putting It Together

In summary, managing for enterprise security is aimed at helping organizations to advance and evolve their security approaches to the degree necessary to ensure that they can achieve and sustain their secure state by

- acculturating the organization to move from a technical view of security to an organizational view
- defining the organization's secure state and the level of security that is "adequate" or in balance between effort and value
- focusing on the organization's critical assets and processes, and the system of internal controls that keeps these assets and processes productive toward accomplishing their missions
- utilizing a set of core operational and organizational capabilities with an expanded focus on security
- mobilizing the collaboration of these capabilities to define a process for managing security at the enterprise level
- measuring the achievement of security goals to ensure continual improvement and optimization

In the next section, four notional approaches to security management are presented that characterize a range of possibilities for an organization. In Section 5, the work performed to date in identifying, developing, and deploying concepts and elements of an enterprise security management approach founded on the fundamental concepts of ESM is presented. Finally, in Section 6, a view of future work aimed at advancing and further codifying these concepts and elements is provided.

4 Notional Approaches to Security Management

Organizations employ many different approaches to security management. The most effective approach for an organization is one that attains and sustains a level of security commensurate with its organizationally driven needs. In Section 2, the shifts in perspective essentially define a range of characteristics of approaches to security management that might be deployed by an organization. On the lower end, the characteristics outline a security approach that tends to be irregular, reactive, and immeasurable; on the contrary, a higher end approach that aims to improve and sustain the organization's resiliency as a goal is characterized by a systematic, continuous, adaptive, and measurable process. Organizations may appropriately fall at either end of this scale or anywhere in between, and the approach that they are using may be entirely adequate to meet their needs.

To serve as a benchmark for our research into an enterprise security management approach, we developed a notional set of approaches to security management. These approaches serve to define four gradations along the range of approaches and the characteristics of each. The nascent thoughts about the value of this scale is that an organization might be able to determine a more appropriate target approach and then take corrective actions to move its current approach toward the target—in essence, move to the right on the scale towards an enterprise security management view of the world.

Much additional work is needed to expand and validate these approaches and is outside of the purpose and intent of this document; we fully expect to review, revise, and expand these notions as our work progresses. However, the sections below provide initial thoughts about each calibration on the scale: ad hoc, vulnerability based, risk based, and enterprise based.

4.1 Ad Hoc

An ad hoc approach to security is characterized by a lack of defined strategy, policies, processes, procedures, or practices. There is little formal responsibility for security in the organization, and security is not specifically included in budgets. The organization tends toward reactive measures, such as when socioeconomic events, viruses, and other widely publicized events occur, and security management activities are applied in discrete, intermittent chunks. Security activities bear little to no alignment with organizational strategic drivers, and when they do, it is by accident. A major symptom of this approach is that the organization is regularly impacted by realized risks that require compensating action to recover from.

4.2 Vulnerability Based

A vulnerability-based approach to security is characterized by primarily focusing on vulnerabilities and reacting to them. It is more proactive than an ad hoc approach in that it is not entirely characterized by incident or event response, and the organization might actually have a plan for addressing security in this way (even if the plan is deficient). Vulnerability-based approaches provide the organization with some ability to detect weaknesses and flaws in software and software configurations and to take action to reduce the likelihood of exploitation. However, this approach is limited by the fact that only known vulnerabilities can be actively managed; no effort is taken to uncover new vulnerabilities and take proactive action or manage the potential impact on the organization if those vulnerabilities are exploited. A vulnerability approach is often technology-centric, tool-driven, and led by the information technology department with little to moderate connection to business drivers and mission. It is focused on information and network security and tends to be paid for as a sunk cost that can't be recovered by the organization. Often, an organization resorts to this approach because of the need to reduce resource (human, financial) strains brought about by the ever-increasing wave of incidents and events.

4.3 Risk Based

An approach to security management based on risk is a significant improvement over ad hoc and reactive approaches.[27] A risk-based approach focuses on the organization's critical assets, particularly information assets that are essential to accomplishing the mission. It takes in the expertise of key managers in the organization to identify and prioritize these assets, define threats, and develop risk mitigation strategies that consider how the organization is impacted if the threats are exploited. Vulnerabilities are important only if they potentially affect critical assets or if they impact the organization. Thus, an *implicit* alignment between security strategies and activities and the organization's strategic drivers is made. A risk-based approach requires a partnership between key subject matter experts and managers in the organization as well as information technology. In highly evolved organizations, a risk-based approach may employ the use of a strategic leader such as a CIO or chief information security officer (CISO) to sponsor the security strategy and ensure connection with other strategic initiatives; in lesser organizations, IT may still lead the charge. Security is an expense-driven activity, but the organization may attempt to identify the benefits it receives, if only because critical assets have been identified and their protection strategies have been re-examined.

[27] The SEI's OCTAVE approach to information security risk assessment focuses in this area. It is available at http://www.cert.org/octave. A risk-based approach to security should be differentiated from risk management performed at the organizational level. A risk-based approach to security refers to the application of risk management principles to the management of security—assessment, mitigation, and monitoring—*not* obtaining security as a byproduct of good enterprise risk management.

4.4 Enterprise Based

An enterprise security management view *explicitly* aligns security strategies with organizational strategies with the aim to achieve, improve, and sustain the organization's resiliency. There is a focus on not only critical assets but also the critical business processes of the organization, as well as the system of internal controls that ensures that these assets and processes remain productive as intended. Security is directed by a c-level executive who is independent of the information technology organization and is involved in the strategic planning for the organization. Security is managed enterprise wide by relying on a set of core capabilities that are found throughout the organization and that contribute to security activities either explicitly or implicitly. There is a strong governance capability to ensure sponsorship and oversight of security activities and alignment to strategic drivers. Excellence in IT operations and services is a major success factor for reaching the organization's secure state. Security is considered an investment, and the organization expects security activities to prove their return to the organization and to be able to be measured.

Appendix B provides a summary of these notional approaches to security management.

5 Progress on Solutions

Our research to date has focused primarily on defining the challenges and barriers that organizations encounter to improving their security efforts and on notionally characterizing a range of approaches that organizations deploy to meet these challenges. Through exploration of the problem, however, we have also been able to begin work on the foundational tools, techniques, and methods that define an enterprise security management approach. This work can be described in the following major areas:

- development of the critical success factors (CSF) method
- standards, practices, and guidelines mapping
- development of a capabilities framework

Each of these areas is described in more detail below.

5.1 Critical Success Factors Methodology

Critical success factors define key areas of performance that are essential for the organization to accomplish its mission. Managers implicitly know and consider these key areas when they set goals and as they direct operational activities and tasks that are important to achieving goals. However, when these key areas of performance are made explicit, they provide a common point of reference for the entire organization. Thus, any activity or initiative that the organization undertakes must ensure consistently high performance in these key areas; otherwise, the organization may not be able to achieve its goals and consequently may fail to accomplish its mission.

In its initial form, the critical success factors method was developed for the purpose of providing a filter that senior executives could apply to prioritize their information needs—essentially to sort out useful information from that which is extraneous and not particularly helpful for decision making. Eventually, the CSF concept found its way into many formalized information and business systems and technology-planning methodologies that are still being used today.

In our work in enterprise security management, the critical success factor method is a fundamental technique for helping organizations to align their security strategies with the organization's strategic drivers and to benchmark, prioritize, and determine the value of any activity (including security) that is performed in the organization. We consider this method one of the initial steps that an organization can take to impart a resiliency focus on their security activities—by providing a target that goes beyond traditional security requirements to organizational requirements. To this end, we fully codified a critical success factor methodology that can be used for enterprise security management [Caralli 04b].

5.2 Affinity Grouping of Standards, Practices, and Guidelines

While we consider our field work and research to form the foundation of our enterprise security management approach, we are also looking to the established community of practice to guide our work in further identifying (and in many cases, confirming) the capabilities that are essential to the process of managing for enterprise security. There is certainly no lack of standards, practices, and guidelines available for information security and related disciplines—in fact, in a recent list of relative documents for information security developed by the Corporate Information Security Working Group, no less than 81 different sets of "best practices" could be found [CISWG 04].

"Best practices" are usually formed out of a need to provide specific guidance on a subject matter area for a particular industry or focus group. In the worlds of technology and security management, there is an ever-increasing number of these best practices being put forth, all in the aim of helping organizations to improve their security effectiveness. In some cases, these practices are embedded in regulations—a way of enforcing a set of best practices through compliance. In our work in enterprise security management, we are not specifically interested in the individual practices so much as the reason for inclusion in the various practice sets. In our opinion, the rationale for inclusion of a particular practice speaks to a capability that is necessary to achieve a desired result. Thus, studying and synthesizing across multiple sets of practices can provide a wealth of information for determining the capabilities that are being recommended to organizations by way of practice sets and regulatory guidelines.

For this reason, we have begun a process of mapping and grouping selected practice sets (via an affinity grouping exercise) to derive a set of capabilities that they represent. In keeping with our view that security management is dependent on many different organizational capabilities (not just focused on security), we have selected practice sets that span a wide range of functions, including IT service and operations management. The following describes each of these practice sets and our rationale for inclusion.

5.2.1 BS7799/ISO17799

BS7799/ISO standard 17799 sets the requirements for an information security management system or process. It is intended to be used by organizations for the identification and management of the range of threats to which information is routinely subjected. The standard is organized into 10 coverage areas: security policy, organization of assets and resources, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, systems development and maintenance, business continuity management, and compliance. For the ESM project, the BS/ISO standard provides valuable input from a security management perspective.

Further information on BS7799 and ISO standard 17799 can be found at http://www.bsi-global.com or http://www.iso.org.

5.2.2 CobiT

CobiT loosely translates to "control objectives for information and related technology." It is issued by the IT Governance Institute (http://www.itgi.org) and promoted by the Information Systems Audit and Control Association (http://www.isaca.org). It has been developed as a general standard for information technology security and control practices and includes a general framework for management, users, IS audit, and security practitioners. CobiT also has a process focus and a governance flavor; that is, management's need to control and measure IT is a focus point. CobiT covers over 30 IT processes in four domains including planning and organization, acquiring and implementing, delivery and support, and monitoring. CobiT also includes a maturity model for IT processes to assist with capability improvement. The intersection between security and IT controls and governance as represented in CobiT is a major focus of the ESM project.

5.2.3 IT Infrastructure Library (ITIL)

The IT Infrastructure Library is a widely accepted collection of best practices for IT service management. It consists of a series of works focused on the delivery of quality IT services and on the environment in which IT operates. It focuses on the growing dependency of organizations on IT to satisfy their missions, which in turn requires high-quality, reliable IT processes.

ITIL is an important ingredient in the ESM work because IT service and operations excellence often translates to higher levels of security and contributes to resiliency. Thus, the inclusion of a model that focuses at the IT service (and service management) level provides another dimension of input to the ESM capabilities that is not directly focused on security yet provides security benefits.

More information on ITIL can be found at http://www.ogc.gov.uk.

5.2.4 Information Security Forum (ISF)

The Information Security Forum is an international association of over 250 leading companies and public sector organizations that fund and cooperate in the development of practical research in information security. The ISF produces the "Standard of Good Practice for Information Security" (The Standard), which is based on 14 years of ongoing research and is positioned as an aid to organizations in understanding and applying best practices for information security. Because it addresses security from a business perspective, The Standard appropriately recognizes the intersection between organizational drivers and security drivers, and thus is a good fit for our work in enterprise security management.

Additional information on the ISF and The Standard can be found at http://www.securityforum.org.

5.2.5 Other Sources

In addition to BS/ISO17799, CobiT, ITIL, and The Standard, we are exploring other guidelines, standards, and practices for inclusion in our mapping exercise. Of note is the inclusion of regulatory guidelines such as the Health Insurance Portability & Accountability Act (HIPAA) (particularly the security standards found at http://www.cms.hhs.gov/hipaa /hipaa2/regulations/security/03-3877.pdf). These guidelines are important because organizations must exhibit security management capabilities that permit them to meet the compliance standards as well as to manage their compliance activities.

Another source of relevant practices is the National Institute of Standards and Technology (NIST) 800-level series on information security. In particular, we are concentrating on NIST 800-14, "Generally Accepted Practices and Principles for Securing Information Systems" (http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf). As we use this information in our work with federal government civilian agencies, we continue to be aware of its influence on the security management processes in organizations, and thus will include relevant NIST 800 documents as necessary.

At the confluence of these various standards, practices, and guidelines we hope to derive (or confirm) a set of capabilities that covers the wide-ranging skill set that is needed to manage security across an enterprise. This includes capabilities for general and IT management, IT service delivery and operations, security, and risk management, as well as representation of sound business practices, such as asset management and business continuity planning. Because security is really about improving and sustaining the organization's resiliency, a multidisciplinary approach that encompasses all of the relevant skills of the organization is needed. It is our belief that, in addition to our research and field work, using varied sources of standards, practices, and guidelines will provide this balance.

In addition to the sources noted above, we also continue to draw on the extensive process management and capability maturity modeling expertise at the SEI. What has been learned in the software engineering realm in the past 15 years (with the development and deployment of the Capability Maturity Model® for Software and now the CMMI® framework) continues to influence process modeling and improvement and is directly applicable to a process-oriented management capability.

Appendix C summarizes these sources and their relevance to enterprise security management.

® Capability Maturity Model and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

5.3 Development of Capabilities and Capabilities Framework

The main focus of our work in enterprise security management is to develop a practical framework that organizations can deploy to enhance, improve, and optimize their ability to manage security as a business process across an enterprise—in essence, a way to move from an ad hoc, reactive approach to one that is systematic, planned, managed, and measured, or to any point in between that is suited to the balance of the organization's security needs and strategic drivers. It is founded on existing security standards, frameworks, and collections of practices (as outlined in Section 5.2) and also considers field work and research with customers and the experiences of high-performing organizations.

The core objectives of the ESM capabilities framework are to

1. describe the essential attributes or capabilities that an organization would be expected to exhibit in order to properly manage and coordinate security efforts at an enterprise level, with an eye toward improving or sustaining the organization's resiliency
2. provide a structure that outlines an evolutionary path from lesser forms of security management to more formalized and disciplined forms that allows for better predictive capabilities in achieving and sustaining an organization's secure state
3. provide a benchmark against which an organization can assess itself to determine what it needs to do to enhance its ability to manage security under complex organizational and technical constraints

The framework is not intended to be a limiting factor or to impose additional best practices on organizations. On the contrary, the framework is meant to be generalized across many different types of organizations, permitting each to define and implement the capabilities using the practices, tools, and methods that are unique to their industry or their specific regulatory constraints. In essence, the framework begins to define an evolutionary path that organizations can use to improve their efforts in managing security across the enterprise.

5.3.1 Notional Set of Capabilities

Our work with customers, research into various standards, practices, and guidelines, and examination of high-performing organizations has yielded a notional set of capabilities—a place to start with the full development of the ESM capabilities framework. In particular, several processes related to IT service delivery and operations appear to show promise as productive mechanisms for improving an organization's security management capabilities.

Table 2 outlines a few examples of the initial capabilities that we have identified.[28] These capabilities form a baseline set from which we will perform additional research (e.g., mapping from best practices) and application in field work.

[28] As our work proceeds, these capabilities will be refined (or even eliminated), additional capabilities will be identified, and the vital connections between the capabilities will be defined. For now, this notional set provides a good point for illustration and productive dialog.

Table 2: Example of ESM Capabilities

Capability or Capability Area	Rationale for Inclusion
Enterprise security governance	Providing the sponsorship and leadership for security management and improvement and monitoring the process for effectiveness
User management	Addressing the control of users of critical assets and processes
Asset management	Identifying, describing, inventorying, and managing the organization's pool of critical assets
Risk management	Applying risk management techniques to drive security goals and objectives
Systems development	Addressing security issues and concerns in earlier stages of an information or technical asset's life cycle (planning, analysis, design, or implementation stages)
IT operations	Obtaining security benefits from optimized IT service and operations delivery, including areas such as release management, configuration management, availability management, and integrity management.

6 Future Work

The future holds much work but great promise for the ability to help organizations make evolutionary improvements in their abilities to manage security as a business process. In this section, we outline our ongoing research and development activities and set the stage for a follow-up technical note that will provide the first glimpse of an ESM capabilities framework.

Future planned work focuses on

- further codification of the critical success factors method and the development of a CSF workshop aimed at ESM
- maturing the ESM concepts, particularly the definition of a "secure state" and a practical means for organizations to define this state as a target for their security efforts
- further development of the ESM capabilities framework, including implementation factors, and a fuller articulation of an ESM approach to security
- development and deployment of an ESM capabilities framework questionnaire
- continued interaction with high-performing organizations
- identification of communities of practice in which to pilot and observe the use of ESM concepts and capabilities
- development of a guiding panel of SEI and community resources
- development of notional metrics to measure success and improvement
- continued research into the concept of organizational resiliency and its role in enterprise security management

Additional detail is provided on selected areas of this work in the following sections. A future technical note is planned that will summarize and present the results of these areas of work.

6.1 Further Development of Capabilities Framework

The primary focus of work from this point forward is the continued development of the ESM capabilities framework. To support this work, we will continue the process of identifying relevant sources of practices, standards, and guidelines and analyzing them to detect and derive additional candidate capabilities.

In addition to further mapping and analysis and the development of the framework, our work in this area also includes

1. asking and answering questions regarding how the capabilities must work together for security management—in essence, determining and describing an enterprise security management process, which will be attempted by applying techniques such as systems dynamics, and which may also tease out additional aspects of the problem
2. asking and answering questions about practical implementation of the framework in organizations (and the scalability of the framework)
3. thoroughly questioning the validity of each capability area and the contribution to security that it provides
4. tying the capabilities to the notional descriptions of each of the four approaches to security management, and asking relevant questions about capabilities and maturity:
    a. Does each approach represent its own set of capabilities? Can the capabilities be assigned to each of the five notional security management approaches?
    b. Is there an implied maturity for process improvement for security management—in other words, does an organization follow a staged approach as it moves through the various approaches on its way to the approach that satisfies the requirements of its secure state?
    c. Is there a continuous representation in the capabilities? Can an organization reach its secure state and sustain it by improving in one or more relevant capability areas rather than moving to higher level approaches?
    d. What factors cause an organization to need to move to a higher, more mature approach? Is it affected by complexity, importance of mission, quality requirements for security, compliance?

In addition to posing these questions, further research into the development of the capabilities framework includes continued refinement and description of the notional approaches to security management (as found in Appendix B), particularly the ESM approach.

6.2 ESM Capabilities Framework Questionnaire

Based on the notional and emerging ESM framework, we plan to develop and deploy an ESM framework questionnaire. This questionnaire will provide us with direct feedback on the effectiveness and degree of insertion of core ESM capabilities in organizations and the direct results of having these capabilities. It will also provide insight into additional capabilities that may not emerge from the practice sets or our field work and research.

6.3 Development of Metrics and Measurement Capabilities

"If you can't measure it, you can't manage it." This is the tune of Peter Drucker and has, over time, been proven as the heart of any process improvement effort, including Six Sigma and CMMI. Measurement is at the heart of any process improvement effort. Nearly all process improvement methodologies identify the ability to measure as one of the most important elements of process quality improvement. Measurement is also a complex and divisive issue, particularly with respect to security goals and objectives. But many have suggested that measurement is one way that security as it is traditionally known will be elevated and made a legitimate enterprise-wide business function. If enterprise security management is about improving the security process and products[29] in organizations, then measurement must be performed.

High-performing organizations are beginning to confront the measurement issue, if only in the context of IT service delivery and operations and the connections to security. For example, they report that they routinely perform the following types of measurement:[30]

- operations performance measures of uptime or downtime, availability, mean time to detect a problem
- security measures of number of incidents, number of vulnerabilities, mean time to detect an incident, number of intrusions
- change management process measures of mean time to repair, mean time between failures, percent of unplanned changes, change rate, change success rate

While these metrics are not security specific, given the impact that IT operations and service delivery has on security, measurements of this type can easily translate into security metrics. They can also have a profound effect on process improvement in that by correcting a process such as change management, the contribution to security is improved.

Further research into security measurement and metrics is a critical component of improving the security approaches and outcomes for organizations and thus forms a major part of our work going forward. In addition to attempting to gather and identify security metrics, this work will also explore the use of popular techniques like Six Sigma to enable and accelerate improvement in core processes and capabilities that form the basis for enterprise security management.

[29] "Products" in this sense refers to the outcomes of the process of managing security in the organization. Improving processes by reducing variability and increasing efficiency generally results in improved products (resulting in a lower defect rate, as is promoted by Six Sigma). These concepts should also translate to the security process in organizations—improvements in the process should result in higher quality security services and products for the organization.

[30] Allen, Julia et al., "Best in Class Security and Operations Roundtable Report," Carnegie Mellon University, Software Engineering Institute, February 2004.

Appendix A Table of Shifts in Perspective

Table 3 is a summary of the shifts in perspective that define a movement toward an enterprise security management and resiliency approach to security.

Table 3: Summary of Shifts in Perspective

Perspective	Shift in Perspective	
Scope • What is the scope and extent of security concern within the organization?	***From*** **technical** ***to*** **organizational**	
	Focus on technical network	Focus on organizational network
	Driven by technical requirements	Driven by organizational requirements
	Protect technical assets	Protect organizational assets
	Technical specialty	Core competency
Ownership • Who has the authority to act? • Who is accountable and responsible?	***From*** **IT** ***to*** **organization**	
	IT as driver, owner, benefactor	Organization as driver, owner, benefactor
	Technical security personnel	Business personnel with security responsibility
	CSO as technical advisor	CSO as advisor to the organization
Focus of security • How is security considered with respect to other organizational requirements?	***From*** **intermittent** ***to*** **integrated**	
	Security singled out for specific attention	Security is a requirement of conducting business
	Security addressed as part of regulatory compliance	Regulatory compliance results from security activities
	Risk management applied to security as a special case	Security results from organization's risk management capabilities

Table 3: Summary of Shifts in Perspective, cont.

Perspective	Shift in Perspective	
Funding for security • How does the organization pay for it? • How does the organization calculate ROI?	**_From_ expense/burden _to_ investment**	
	Benefit not measured, hard to measure	Benefit measured, results documented
	ROI not required or quantifiable	ROI required and quantifiable
	Security goals ambiguous	Security goals specific
Drivers • How is the approach implemented? • What drives the approach?	**_From_ external _to_ internal**	
	Reliance on community best practices; little to no consideration of organizational drivers	Practice selection driven by organizational requirements
	Technology/practice-centric	Process-centric
Approach and management • What is our approach to managing security? • How well equipped and capable are we?	**_From_ ad hoc/tactical _to_ managed/strategic**	
	Security viewed as protective, defensive	Security viewed as enabling
	React to complexity and dynamic risk environment	Adapt to complexity and dynamic risk environment
	Accidental, intermittent	Planned, defined, repeatable, sustainable
	Monitoring after the fact	Sensing in advance
	Rewards/reinforcement for individual skill, heroics	Rewards/reinforcement for consistency, discipline

Appendix B Four Notional Approaches to Security Management

Table 4 summarizes and highlights four notional approaches to security management. These stages were developed through field work and research and provide the basis for continuing research into the maturity of approaches to managing enterprise security.

Table 4: Four Notional Approaches to Security Management

Characteristic	Approach			
	Ad hoc	Vulnerability based	Risk based	Enterprise based
Focus	Incidents or events	Vulnerabilities	Critical assets	Critical assets and processes, and strategic drivers, aiming at organizational resiliency
Responsibility	Unassigned or left to heroes who step up to the challenge	Generally IT department	Key organizational managers, CIO, CISO, and sometimes IT, or a blend of these	C-level executives, CSO, everyone in the organization
Major activities	Responding to events	Identifying vulnerabilities and implementing mitigating actions	Identifying threats to key assets and implementing mitigating actions	Managing security through a process dependent on organizational capabilities that are not necessarily focused on traditional security
Funding	Expense No measurement	Expense No measurement	Expense Qualitative measurement	Strategic, budgeted, capitalized, investment Qualitative and quantitative measurement

Table 4: Four Notional Approaches to Security Management, cont.

Characteristic	Approach			
	Ad hoc	**Vulnerability based**	**Risk based**	**Enterprise based**
Alignment to strategic organizational drivers	None	Little to none	Implicit	Explicit
Dependencies	People; heroics	People; catalog(s) of vulnerabilities	Dependent on localized risk management (not enterprise wide), operational context, catalog(s) of practices	Capabilities, other indicators of organizational health—system of internal controls, IT service and operations excellence, etc.
Governance structure	None	None or informal	Informal; may include involvement of chief risk officer or other c-level executive	Formal; governance is a primary function and capability

Appendix C Sources of Best Practices

Table 5 summarizes the sources being used as input to the development of the capabilities framework and their relevance to enterprise security management.

Table 5: Sources for ESM Capabilities

Source	Audience	Focus	Relevance to ESM
BS7799/ISO17799	International	Information security management	Management of information security practices
COBIT	International	IT security and control	Control objectives for information technology security and process control
ITIL	International	IT service management	IT service and operations management practices that contribute to security
ISF-The Standard	International	Information security	Information security practices
NIST 800-14	Mostly U.S.	Information systems security	Information security practices that are focused on systems
HIPAA	U.S.	Data security	Information security practices that are focused on information and data
CMMI & other maturity models	International	Process improvement	Structure for process improvement and maturity

References

URLs are valid as of the publication date of this document.

[Alberts 01] Alberts, Christopher J. & Dorofee, Audrey J. *OCTAVE Criteria V2.0* (CMU/SEI-2001-TR-016, ADA3399229). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. http://www.sei.cmu.edu/publications/documents/01.reports/01tr016.html.

[Allen 02] Allen, Julia & Sledge, Carol. "Information Survivability: Required Shifts in Perspective." *CrossTalk*, July 2002. http://www.stsc.hill.af.mil/crosstalk/2002/07/allen.html.

[Allen 04] Allen, Julia. *Governing for Enterprise Security*. http://www.cert.org/governance/ges.html.

[Behr 04] Behr, Kevin; Kim, Gene; & Spafford, George. *The Visible Ops Handbook*. Eugene, OR: Information Technology Process Institute, June 2004.

[Berinato 04] Berinato, Scott. "Locked Out." *CSO Online*, July 2004. http://www.csoonline.com/read/070104/cisco.html.

[Booz 04] Starr, Randy; Newfrock, Jim; & Delurey, Michael. "Enterprise Resilience: Managing Risk in the Networked Economy." *Strategy & Business*, Spring 2003. http://www.strategy-business.com.

[Caralli 04a] Caralli, Richard & Wilson, William. *The Challenges of Security Management*. http://www.cert.org/archive/pdf/ESMchallenges.pdf (2004).

[Caralli 04b] Caralli, Richard. *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management* (CMU/SEI-2004-TR-010). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/publications/documents/04.reports/04tr010.html.

[CISWG 04] Corporate Information Security Working Group. *Information Security Management References*. Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives, March 18, 2004. http://reform.house.gov/UploadedFiles/Best Practices Bibliography.pdf.

[GE 04] General Electric Co. *The Roadmap to Customer Impact.* http://www.ge.com/sixsigma.

[Gremba 97] Gremba, Jennifer & Myers, Chuck. "The IDEAL Model: A Practical Guide for Improvement." *Software Engineering Institute Bridge*, 1997. http://www.sei.cmu.edu/ideal/ideal.bridge.html.

[Hamel 03] Hamel, Gary & Valinkangas, Liisa. "The Quest for Resilience." *Harvard Business Review 81*, 9 (September 2003). http://www.hbr.org.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY
(Leave Blank)

2. REPORT DATE
December 2004

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
Managing for Enterprise Security

5. FUNDING NUMBERS
F19628-00-C-0003

6. AUTHOR(S)
Richard A. Caralli

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER
CMU/SEI-2004-TN-046

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQ ESC/XPK, 5 Eglin Street, Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

Security has become one of the most urgent issues for many organizations. It is an essential requirement for doing business in a globally networked economy and for achieving organizational goals and mission. But it is no small task. The technical and environmental complexity of today's organizations and the ever-increasing dependence on technology to drive and automate processes and create competitive advantages make security a challenging activity. Adding to this complexity is a growing list of vulnerabilities and increasingly sophisticated threats to which organizations are subjected on a daily basis.

Organizations can no longer be effective in managing security from the technical sidelines. Security lives in an organizational and operational context, and thus cannot be managed effectively as a stand-alone discipline. Because security is a business problem, the organization must activate, coordinate, deploy, and direct many of its existing core competencies to work together to provide effective solutions. And to sustain success, security at an enterprise level requires that the organization move toward a security management process that is strategic, systematic, and repeatable—in other words, efficient at using security resources and effective at meeting security goals on a consistent basis. Managing for enterprise security defines a disciplined and structured means for realizing these objectives.

This report presents the interim results of work done by members of the Networked Systems Survivability Program at the Software Engineering Institute in exploring these issues. The authors offer a view of the changing environment in which security must be performed and, from their field work and research, itemize characteristics of common existing approaches to security that limit effectiveness and success. A "desired state" as a security target for the organization is outlined, and the organizational transformation that the authors believe is essential for approaching security as a business problem is presented. Finally, the authors describe their current work in exploring solutions that they believe will enable this transformation.

14. SUBJECT TERMS
enterprise security management, strategic planning, information security, risk management

15. NUMBER OF PAGES
55

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
UL